(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 810 138**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **00 07318**

(51) Int Cl[7] : **G 06 K 19/073**, G 06 F 12/14

# (12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 08.06.00.

(30) **Priorité** :

(43) **Date de mise à la disposition du public de la demande** : 14.12.01 Bulletin 01/50.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *BULL CP8 Société anonyme* — FR.

(72) **Inventeur(s)** : FOUGEROUX NICOLAS, HAMEAU PATRICE et BOLE BENOIT.

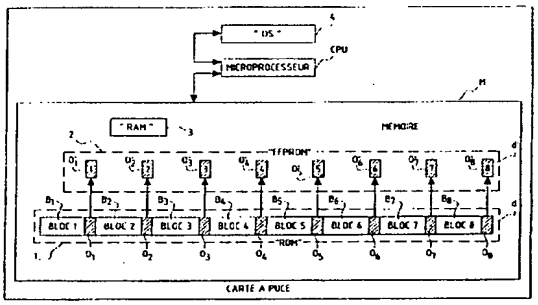
(73) **Titulaire(s)** :

(74) **Mandataire(s)** : CP8 TECHNOLOGIES.

## (54) PROCEDE DE STOCKAGE SECURISE D'UNE DONNEE SENSIBLE DANS UNE MEMOIRE D'UN SYSTEME EMBARQUE A PUCE ELECTRONIQUE, NOTAMMENT D'UNE CARTE A PUCE, ET SYSTEME EMBARQUE METTANT EN OEUVRE LE PROCEDE.

(57) L'invention concerne un procédé d'enregistrement sécurisé d'une donnée dite sensible, par exemple d'une clé de chiffrage, dans une mémoire (M) d'un système embarqué à puce électronique, notamment d'une carte à puce (CP). La mémoire (M) comprend deux organes de stockage physiquement distincts (1, 2), par exemple une mémoire fixe de type " ROM " (1) et une mémoire re-programmable de type " EEPROM " (2). La donnée sensible est scindée en au moins deux parties (d, d'), selon une configuration logique déterminée, chacune de ces parties étant enregistrée dans un des organes de mémoire distinct (1, 2). Une donnée supplémentaire de vérification, somme de contrôle ou donnée de hachage, peut être enregistrée en supplément dans le premier organe de mémoire (1), en même temps que la première partie de donnée sensible (d).

L'invention concerne également un système embarqué à puce électronique, notamment une carte à puce (CP).




FR 2 810 138 - A1

L'invention concerne un procédé d'enregistrement sécurisé de données sensibles dans une mémoire d'un système embarqué à puce électronique.

Elle s'applique plus particulièrement à une carte à puce.

L'invention concerne encore un système embarqué pour la mise en œuvre du procédé.

Dans le cadre de l'invention, le terme "système embarqué" vise des systèmes ou dispositifs divers ayant en commun le fait de disposer d'une puce électronique comprenant des moyens de mémoire et de traitement de données, généralement constitués par un microprocesseur ou un microcontrôleur. Un tel système embarqué peut être constitué notamment par une carte à puce.

De même, le terme "sensible" doit être compris dans son sens le plus général. Il concerne toutes sortes de données secrètes ou pour le moins confidentielles, notamment des algorithmes de chiffrage, des clés secrètes de chiffrage , des données d'identification ou des informations à caractère secret, etc., stockées dans une ou plusieurs types de mémoires dont sont munies les cartes à puce. Ce type de données sera appelé ci-après "secret", de façon générique.

L'invention s'applique encore plus particulièrement, mais non exclusivement, au stockage de clés secrètes stockées en vu d'être utilisées pour la pré-initialisation sécurisée de cartes à puce. Il est en effet bien connu que des fonctions relatives à la sécurité sont dévolues aux cartes à puce. Là encore le terme sécurité doit être entendu dans un sens large. Ce terme recouvre en effet divers concepts : confidentialité, authentification, etc.

Ci-après, pour fixer les idées et sans que cela limite en quoi que ce soit sa portée, on se placera dans ce cas d'application préférée de l'invention, sauf mention contraire.

De façon habituelle, dans l'art connu, les secrets contenus dans les cartes à puce sont stockés linéairement dans une même zone de mémoire. En particulier, les secrets sont stockés dans des mémoires fixes à lecture

seule ("ROM", pour "Read-Only Memory") ou semi-fixes, c'est-à-dire re-programmable par effacement électrique à lecture seule, par exemple de type dit "EEPROM" ("Electrically Erasable Programmable Read-Only Memory"). Or, les mémoires des puces électroniques sont la proie de fraudeurs et les attaques que l'on peut constater sont de plus en plus nombreuses et sophistiquées.

En particulier, le "dumping" ("vidage" ou copie de la mémoire) de la mémoire "ROM" est un souci constant pour les cartes à puce.

Les mémoires de type "EEPROM", contenant traditionnellement des données dites sensibles, sont sujettes à la plupart des agressions connues à l'heure actuelle.

L'invention vise à pallier les inconvénients des dispositifs de l'art connu, et dont certains viennent d'être rappelés.

L'invention se fixe pour but un procédé de stockage sécurisé de données sensibles dans la mémoire d'une carte à puce, et de façon plus générale dans la mémoire d'un système embarqué à puce électronique.

Elle concerne également un système embarqué à puce électronique pour la mise en œuvre de ce procédé. La puce électronique comprend des moyens de mémoire et de traitement de données, généralement sous la commande d'un système d'exploitation (ou "OS", pour "Operating System", selon la terminologie anglo-saxonne).

Pour ce faire, selon une caractéristique avantageuse, le secret est "éclaté" physiquement et logiquement dans plusieurs moyens de mémoire dont est munie la puce électronique.

Dans un mode de réalisation avantageux, la mémoire de ladite puce électronique est divisée en deux parties distinctes, la première étant constituée par une mémoire de type "ROM", de façon plus générale une mémoire fixe à lecture seule, la seconde partie étant constituée par une mémoire de type "EEPROM", de façon plus générale une mémoire semi-fixe re-programmable.

Selon une première variante du procédé de l'invention, un même secret est "éclaté" entre deux parties de mémoire ou plus, physiquement distinctes.

En particulier, dans le domaine d'application préféré de l'invention, le procédé permet l'authentification d'une carte à puce en phase de pré-initialisation, lorsque la partie de mémoire de type "EEPROM" est encore vierge de données, en dehors de celles programmées par une entité que l'on appellera ci-après "fondeur".

Dans le cadre de l'invention, le terme "pré-initialisation" s'entend dans un sens général. Il est notamment relatif à la phase de fabrication d'une carte à puce traditionnelle ou à la phase précédant la phase d'initialisation d'une carte à puce dite ouverte.

Selon un mode de réalisation avantageux encore, la majeure partie des données constituant le secret est stockée en mémoire "ROM". Seule une faible partie de ces données est stockée en mémoire "EEPROM".

Selon cette caractéristique supplémentaire de l'invention, une clé secrète est alors contenue dans la partie de mémoire de type "ROM", dans sa très grande majorité. Il suffit au fondeur d'écrire une partie plus réduite de la clé secrète dans la partie de mémoire de type "EEPROM" pour que le système d'exploitation précité puisse disposer de la clé secrète dans sa totalité. Du fait de son stockage particulier, il est à noter que la clé secrète est envoyée en deux parties à deux services distincts chez le fondeur, ce qui permet de réduire les risques de fraude lors du transfert de secret.

Ce stockage particulier permet donc de minimiser le nombre d'octets programmés sous pointe par le fondeur et présente en conséquence l'avantage de réduire les coûts de fabrication. En effet, pour garantir un haut degré de sécurité, les clés actuellement utilisées sont de grande longueur. On peut donc alléger le stockage de ces clés de grande longueur, habituellement effectué en "EEPROM", en en déportant la plus grande partie dans la "ROM".

Selon une seconde variante de réalisation, un premier secret est stocké dans une première partie de la mémoire et un ou plusieurs autres

secrets, dérivé(s) du premier secret, directement ou indirectement, est(sont) stocké(s) dans au moins une autre partie de mémoire physiquement distincte. Ce ou ces secret(s) supplémentaire(s) peuvent être obtenu(s) avantageusement par chiffrage.

A titre d'exemple, dans un domaine d'application typique du procédé selon l'invention, une clé de chiffrage (symétrique) est présente dans une première zone de mémoire d'une carte à puce, de type "ROM", au moment du masquage de celle-ci. Une information confidentielle est stockée dans une seconde zone de mémoire, de type "EEPROM", lors de l'utilisation de la carte à puce. Cette information est chiffrée (par exemple à l'aide de l'algorithme dit triple "DES") avec la clé de chiffrage précitée présente dans la zone "ROM". Cette méthode présente un grand intérêt. En effet, en sus de la protection contre le "dumping" de la mémoire, on constate que l'information est également protégée lorsqu'elle est écrite dans la carte à puce. Même l'entité qui "écrit" la clé ne la connaît pas.

De ce qui précède, il s'ensuit que, quel que soit le mode de réalisation, ou les variantes considérées de ces modes de réalisation, une attaque frauduleuse réussie d'une des parties de la mémoire ne peut conduire à la connaissance complète du secret. Dans la réalité, et dans la mesure où la répartition des éléments du secret entre les parties distinctes de la mémoire est réalisée de façon judicieuse, la connaissance partielle du secret acquise de façon frauduleuse ne permettra jamais de retrouver ultérieurement le secret, par exemple en tentant un décryptage à l'aide de traitements mathématiques appropriés, ce qui permettrait de déduire le secret complet de la connaissance partielle précitée. Cette répartition judicieuse est, en soi, à la portée de l'homme de métier. On pourra donc considérer que l'attaque a finalement échoué.

En outre, comme il le sera montré ci-après de façon plus détaillée, il est possible d'associer le procédé de l'invention à des dispositions de vérification, d'authentification et/ou de chiffrage, connues en soi, mais dont le degré de sécurité obtenu est renforcé grâce aux dispositions propres à l'invention.

L'invention a donc pour objet principal un procédé d'enregistrement sécurisé d'une donnée dite sensible dans une mémoire d'un système embarqué à puce électronique comprenant aux moins deux moyens de mémoire physiquement distincts, caractérisé en ce que ladite donnée sensible est scindée en au moins deux parties, selon une configuration logique déterminée, et en ce que chacune desdites parties scindées est enregistrée dans un desdits moyens de mémoire physiquement distincts.

L'invention a encore pour objet un système embarqué à puce électronique pour la mise en œuvre de ce procédé.

L'invention va maintenant être décrite de façon plus détaillée en se référant aux dessins annexés, parmi lesquels :

- la figure 1 illustre schématiquement un exemple de configuration de la mémoire d'une carte à puce selon un aspect de l'invention, pour une application du procédé à l'enregistrement d'une clé secrète ; et
- la figure 2 illustre schématiquement une variante de réalisation de la configuration de la mémoire d'une carte à puce de la figure 1.

Comme il a été indiqué dans le préambule de la présente description, on se placera ci-après dans le cadre de l'application préférée de l'invention, c'est-à-dire dans le cas de la sécurisation de la phase de pré-initialisation d'une carte à puce.

De façon plus précise, on va illustrer le procédé selon l'invention dans son application au stockage d'une clé secrète asymétrique que l'on référencera ci-après *d*. Cette clé *d* peut permettre à une carte à puce de générer un cryptogramme à partir d'un algorithme asymétrique approprié. Ce cryptogramme, s'il est retourné à un terminal d'authentification de la carte à puce, peut servir à l'authentification de celle-ci.

La figure 1 illustre, de façon schématique, un exemple d'architecture de carte à puce *CP*. Cette dernière comprend une mémoire *M*, elle-même constituée dans l'exemple décrit, d'une mémoire vive à accès aléatoire de type dit "RAM" (pour "Random Access Memory") 3 et d'une mémoire non volatile comprenant une partie fixe 1, de type "ROM", et une

partie semi-fixe 2, de type "EEPROM" ou similaire. La carte à puce *CP* comprend en outre des moyens de traitement de données, par exemple un microprocesseur référencé *CPU*, coopérant avec un système d'exploitation 4. Le système d'exploitation est une pièce de logiciel constituée d'une suite de microinstructions qui peuvent être stockées en tout ou partie dans la zone "ROM" 1 et/ou la zone "EEPROM" 2 de la mémoire *M*.

Selon une des caractéristiques de l'invention, le stockage de la clé *d* est effectué dans, au moins, deux parties physiquement distinctes de la mémoire *M*. De façon plus précise, dans l'exemple illustré, le stockage de cette clé *d* est effectué dans une partie non volatile de la mémoire *M* : une partie en mémoire fixe 1, de type "ROM", et une partie en mémoire semi-fixe 2, de type "EEPROM" ou similaire.

La clé secrète *d* se compose donc d'une partie en "ROM" 1, présente avant l'arrivée chez l'entité que l'on a appelé "fondeur", et d'une partie écrite lors d'une opération dite "sous pointe" par ce dernier, en "EEPROM" 2. Les octets programmés en "EEPROM" 2 sont des données extrêmement sensibles, traitées comme des octets de sécurité. Ceci implique bien sûr que la clé secrète *d* soit déjà connue à l'heure du masquage.

A titre d'exemple, pour fixer les idées, on va considérer ci-après une clé secrète *d* de 1024 bits (soit 128 octets).

Dans un mode de réalisation préféré du procédé de l'invention, la clé *d* réside totalement en "ROM" 1, mais certains octets sont faux ou altérés. A titre d'exemple, un octet par bloc de seize octets est faux, une valeur erronée ayant été volontairement écrite dans le code "ROM".

On a représenté sur la figure 1 les différents blocs de la clé *d* sous les références $B_1$ à $B_8$. Les octets erronés sont référencés $O_1$ à $O_8$. Les valeurs correctes des octets référencés, $O'_1$ à $O'_8$, sont stockées en "EEPROM" 2, sous la forme également de huit octets correspondants. Ces octets, $O'_1$ à $O'_8$, forment une clé partielle *d'*.

Dans cet exemple, huit octets (soit 128/16 = 8) doivent donc être programmés en "EEPROM" 2. Mais on doit bien comprendre que le

stockage en "EEPROM" 2 peut être quelconque, le système d'exploitation 4, coopérant avec les moyens de traitement de données *CPU* se chargeant de la reconstitution en "RAM" 3 de la clé complète exacte, que l'on peut appeler $d'$, lors de son utilisation. Cette reconstitution s'effectue, dans l'exemple décrit, simplement par substitution des octets corrects, $O'_1$ à $O'_8$, aux octets erronés, $O_1$ à $O_8$.

On constate donc que la connaissance d'une des clés, soit $d$, soit $d'$, par quel que moyen que ce soit, notamment par les opérations frauduleuses de "dumping" précitées, ne permet pas d'en déduire le "secret total", c'est-à-dire la clé correcte complète $d'$.

Comme il a été rappelé, les clés, pour obtenir une bonne sécurité sont généralement longues, par exemple 128 octets ou 1024 bits comme indiqué ci-dessus. Le procédé selon l'invention, outre le degré de sécurité qu'il apporte, permet de ne devoir enregistrer en "EEROM" 2 qu'une fraction très réduite de la clé totale $d$, soit 8 octets ou 64 bits. Seule cette fraction de clé doit être écrite sous "pointe" par le fondeur, ce qui présente un avantage important, car cette opération est longue et coûteuse.

On doit bien comprendre que de nombreuses autres configurations de répartition de la clé entre les deux types de mémoire, "ROM" 1 et "EEPROM" 2, sont possibles. Les deux séries d'octets doivent seulement être en correspondance biunivoque. Cependant, l'homme de métier doit veiller à ce que cette répartition ne permette pas que la connaissance d'une des deux clés partielles : $d$ (ayant la même longueur que la clé totale correcte $d'$, mais en partie "altérée") ou $d'$, autorise, par des méthodes mathématiques ou autres, la déduction de la clé totale, à partir de cette connaissance partielle. La répartition qui vient d'être décrite en regard de la figure 1, pour les longueurs de clés considérées, satisfait cette exigence.

Dans une variante de réalisation supplémentaire du procédé de l'invention, en vue d'augmenter encore le degré de sécurité obtenu, on prévoit le stockage en "ROM" 1 d'une donnée d'information permettant de garantir l'intégrité de la clé secrète $d$ et, donc, de préserver dans le temps l'intégrité des mémoires "ROM" 1 et "EEPROM" 2. Cette donnée peut

prendre la forme d'un calcul de somme de contrôle sur la clé secrète, connu sous l'appellation anglo-saxonne de "checksum". Cette donnée peut encore être obtenue à l'aide d'une fonction de hachage ou "hash" de cette même clé. Pour ce faire, dans ce dernier cas, il est utilisé avantageusement un algorithme du type connu sous le sigle "SHA-1". Cet algorithme particulier doit donc être implanté dans la carte à puce. Le résultat de cette fonction de hachage a une longueur de 160 bits. L'opération initiale permettant d'obtenir ladite donnée est concomitante à l'enregistrement de la clé *d* dans la "ROM" 1.

Le "checksum" ou le "hash" est effectué à chaque utilisation de la clé secrète et comparé à la donnée d'information enregistrée dans la mémoire "ROM" 1.

La figure 2 illustre schématiquement l'architecture d'une carte à puce *CP* stockant une telle donnée de "hash" en mémoire "ROM" 1. Les éléments communs à la figure 1 portent les mêmes références et ne seront re-décrits qu'en tant que de besoin.

La donnée *H* est stockée en "ROM" 1 et vérifiée à chaque utilisation de la clé afin de préserver l'intégrité des zones mémoire "ROM" 1 et "EEPROM" 2. Cette vérification s'effectue sous la commande des moyens de traitement de données *CPU* et de programmes enregistrés dans la mémoire.

Jusqu'à ce stade de la description, il a été supposé, au moins implicitement, que les données secrètes réparties entre les deux parties physiquement distinctes de la mémoire *M* constituaient un même et unique secret.

Dans une variante supplémentaire du procédé selon l'invention, les données secrètes stockées en mémoire "ROM" 1 peuvent constituer un premier secret. Des deuxièmes données secrètes, dérivées des premières données secrètes, peuvent constituer un deuxième secret. Ces données, selon une des caractéristiques de l'invention, sont alors stockées dans une deuxième partie physiquement distincte de la mémoire *M*, par exemple en "EEPROM" 2. Ces données peuvent avantageusement être obtenues par chiffrage des premières données, par utilisation de tout algorithme

approprié, de type symétrique ou non. On peut considérer que le secret est bien "partagé" ou "scindé", au sens du procédé selon l'invention, qu'il ne peut être déduit de la connaissance d'une seule partie de la mémoire *M*.

A la lecture de ce qui précède, on constate aisément que l'invention atteint bien les buts qu'elle s'est fixés.

Elle permet un grand degré de sécurité pour le stockage de données sensibles, telles des clés ou similaire, en les répartissant physiquement dans au moins deux parties physiquement distinctes de la mémoire d'une carte à puce, et de façon plus générale d'un système embarqué à puce électronique.

Il doit être clair cependant que l'invention n'est pas limitée aux seuls exemples de réalisations explicitement décrits, notamment en relation avec les figures 1 et 2.

On peut notamment répartir les données secrètes dans plus de deux parties de mémoire physiquement distinctes. De même, lorsque les données réparties ne représentent pas un même et unique secret, le nombre de secrets dérivés du premier peut être supérieur à l'unité. On peut également dériver des secrets en cascade et les enregistrer séparément dans des parties de mémoires physiquement distinctes.

L'invention n'est pas non plus limitée à l'application d'authentification de la phase de pré-initilisation d'une carte à puce qui a été évoquée de façon plus détaillée. Elle s'applique toutes les fois qu'une donnée sensible, clé de chiffrage ou autre, doit être stockée dans la mémoire d'un système embarqué.

## REVENDICATIONS

1. Procédé d'enregistrement sécurisé d'une donnée dite sensible dans une mémoire d'un système embarqué à puce électronique comprenant aux moins deux moyens de mémoire physiquement distincts, caractérisé en ce que ladite donnée sensible est scindée en au moins deux parties (d, d'), selon une configuration logique déterminée, et en ce que chacune desdites parties scindées (d, d') est enregistrée dans un desdits moyens de mémoire physiquement distincts (1, 2).

2. Procédé selon la revendication 1, caractérisé en ce que, ladite donnée sensible étant scindée en au moins deux parties (d, d'), elle constitue un secret unique et en ce que chacune desdites parties scindées est enregistrée dans un desdits moyens de mémoire physiquement distincts (1, 2).

3. Procédé selon la revendication 1, caractérisé en ce que ladite donnée sensible étant scindée en au moins deux parties (d, d'), ladite première partie (d) constitue un premier secret et chacune desdites parties supplémentaires (d') sont dérivées de ladite première partie (d) pour constituer des secrets supplémentaires, et en ce que chacune desdites parties scindées est enregistrée dans un desdits moyens de mémoire physiquement distincts (1, 2).

4. Procédé selon la revendication 1, caractérisé en ce que ladite donnée sensible est un mot binaire de longueur égale à un nombre déterminé d'octets et est scindée de façon à être enregistré dans deux moyens de mémoire physiquement distincts (1, 2), en ce qu'une première partie est un premier mot binaire (d) constitué de blocs d'octets ($B_1$-$B_8$), de même longueur que ladite donnée sensible, en ce que cette première partie (d)

comporte une suite d'octets corrects et d'octets altérés ($O_1$-$O_8$), répartis dans ledit mot (d) selon une configuration prédéterminée, en ce que ladite seconde partie est un second mot binaire (d'), de longueur égale au nombre desdits octets altérés ($O_1$-$O_8$) et constitué d'octets ($O'_1$-$O'_8$) en correspondance biunivoque avec lesdits octets altérés ($O_1$-$O_8$), de manière à pouvoir corriger ces octets altérés ($O_1$-$O_8$) et à reconstituer ladite donnée sensible à partir desdites première (d) et seconde parties (d').

**5.** Procédé selon la revendication 4, caractérisé en ce que ladite donnée sensible est une clé de chiffrage.

**6.** Procédé selon la revendication 1, caractérisé en ce que, ladite donnée sensible étant scindée en des première (d) et seconde parties (d'), enregistrées respectivement dans des premier (1) et second (2) moyens de mémoire physiquement distincts, il est procédé à une opération, concomitante à l'enregistrement de ladite première partie (d), dite de hachage de ladite donnée sensible dont le résultat se présente sous la forme d'une donnée d'information (H), en ce que ladite donnée d'information (H) est enregistrée dans lesdits premiers moyens de mémoire (1), et en ce qu'il comprend une lecture de ladite donnée d'information (H), une opération supplémentaire de hachage de ladite donnée sensible et une comparaison entre ladite donnée d'information lue et le résultat de ladite opération de hachage supplémentaire lors de chaque utilisation de ladite donnée sensible, de manière à en certifier l'intégrité.

**7.** Procédé selon la revendication 6, caractérisé en ce que ladite opération de hachage est obtenue par l'application sur ladite donnée sensible de l'algorithme de hachage dit "SHA-1".

**8.** Système embarqué à puce électronique muni de moyens de mémoire pour l'enregistrement d'au moins une donnée dite sensible, lesdits moyens de mémoire comprenant au moins deux organes de mémoire physiquement distincts, caractérisé en ce que ladite donnée sensible étant scindée en au moins deux parties (d, d') de configurations déterminées, chacun desdits organes de mémoire (1, 2) enregistre l'une desdites parties de donnée sensible (d, d').

**9.** Système selon la revendication 8, caractérisé en ce que lesdits moyens de mémoire (M) comprennent un premier organe de mémoire fixe à lecture seule, de type dit "ROM" (1), et un deuxième organe de mémoire re-programmable par effacement par voie électrique à lecture seule, de type dit "EEPROM" (2), et en ce que chacun desdits premier (1) et deuxième (2) organes de mémoire enregistre une desdites parties (d, d') scindées de ladite donnée sensible.

**10.** Système selon la revendication 8, caractérisé en ce qu'il est constitué par une carte à puce (CP).

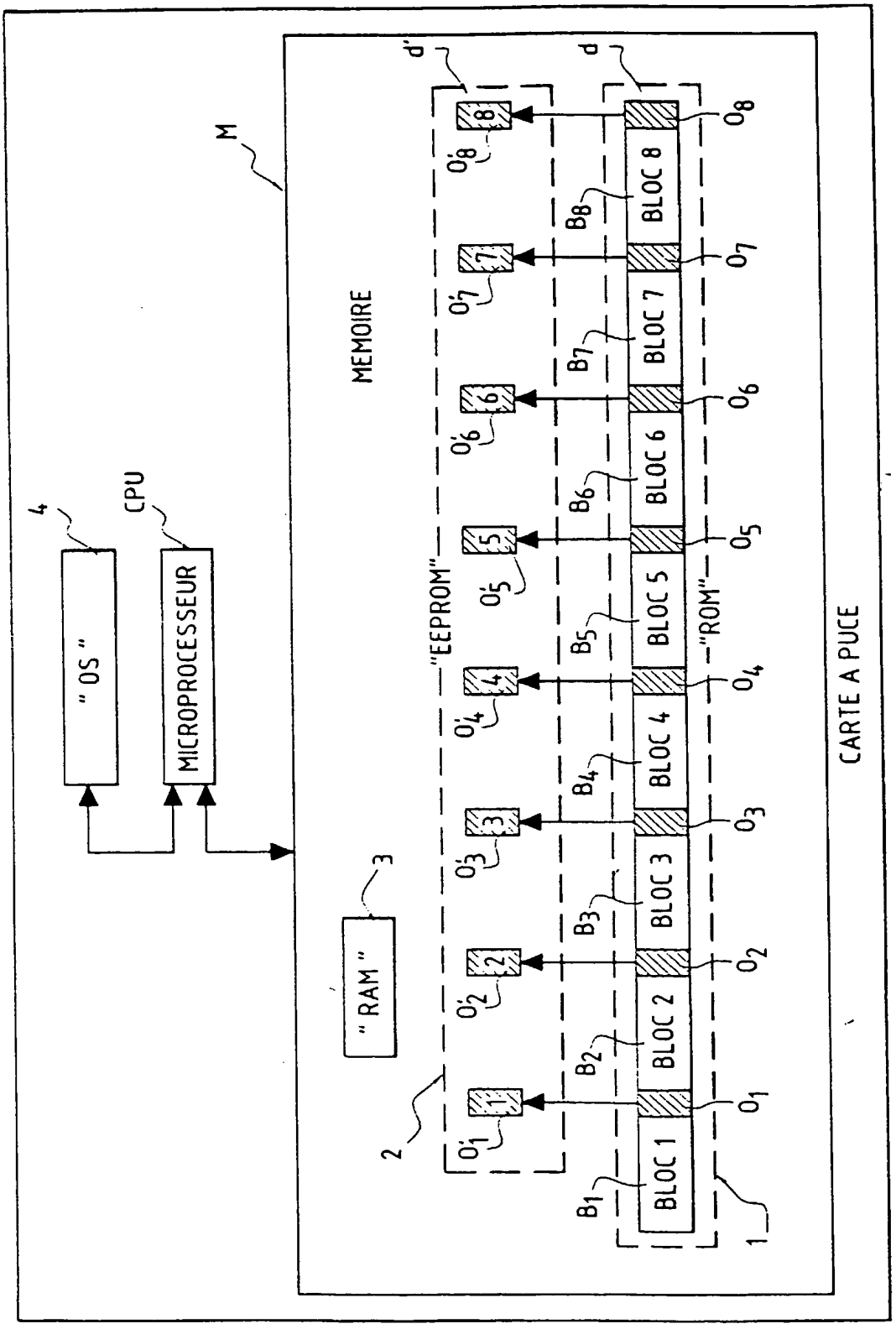

M
MEMOIRE
CARTE A PUCE
"EEPROM"
"ROM"
" OS "
MICROPROCESSEUR
CPU
" RAM "
BLOC 1
BLOC 2
BLOC 3
BLOC 4
BLOC 5
BLOC 6
BLOC 7
BLOC 8

FIG.1

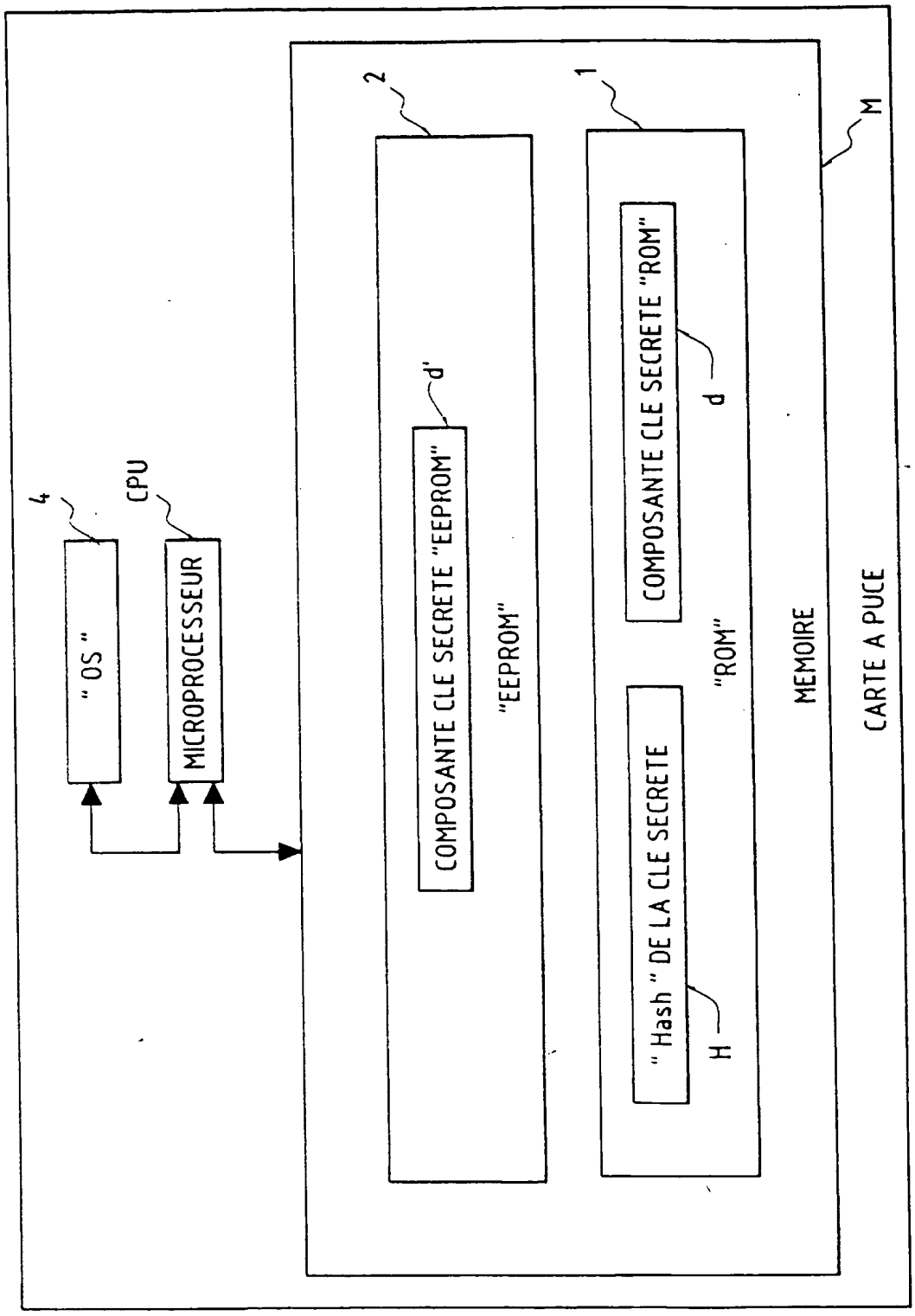

CARTE A PUCE
MEMOIRE
M
"EEPROM"
2
COMPOSANTE CLE SECRETE "EEPROM"
d'
"ROM"
1
COMPOSANTE CLE SECRETE "ROM"
d
"Hash" DE LA CLE SECRETE
H
CPU
MICROPROCESSEUR
4
" OS "

FIG.2

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

# RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2810138

N° d'enregistrement national

FA 593819
FR 0007318

| DOCUMENTS CONSIDÉRÉS COMME PERTINENTS | | Revendication(s) concernée(s) | Classement attribué à l'invention par l'INPI |
|---|---|---|---|
| Catégorie | Citation du document avec indication, en cas de besoin, des parties pertinentes | | |
| X | US 5 467 081 A (DREWS ET AL.)<br>14 novembre 1995 (1995-11-14) | 1-3,8,10 | G06K19/073<br>G06F12/14 |
| A | * colonne 1, ligne 53 - colonne 5, ligne 33 *<br>* colonne 5, ligne 66 - colonne 10, ligne 11; figures 1-5B * | 4-6,9 | |
| Y | US 5 623 546 A (HARDY ET AL.)<br>22 avril 1997 (1997-04-22) | 1-3,5,8, 10 | |
| A | * colonne 2, ligne 38 - colonne 9, ligne 39; figures 1-3 * | 4,6,7,9 | |
| Y | US 5 150 407 A (CHAN)<br>22 septembre 1992 (1992-09-22)<br>* colonne 2, ligne 31 - ligne 56 *<br>* colonne 3, ligne 14 - colonne 8, ligne 25; figures 1,2 * | 1-3,5,8, 10 | |
| A | WO 98 52160 A (MONDEX INTERNATIONAL LIMITED) 19 novembre 1998 (1998-11-19)<br>* page 5, ligne 10 - ligne 18 *<br>* page 7, ligne 9 - page 17, ligne 16; figures 1-5 * | 1,8 | |
| A | US 5 159 183 A (YAMAGUCHI)<br>27 octobre 1992 (1992-10-27)<br>* colonne 2, ligne 48 - ligne 68 *<br>* colonne 3, ligne 26 - colonne 5, ligne 18; figures 1-5 * | 1,8 | |
| A | US 5 553 144 A (ALMQUIST ET AL.)<br>3 septembre 1996 (1996-09-03)<br>* colonne 3, ligne 29 - colonne 10, ligne 14; figures 1-7B * | 1,8 | |
| | -/-- | | |

| DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7) |
|---|
| G07F<br>G06K<br>G06F |

2

| Date d'achèvement de la recherche | Examinateur |
|---|---|
| 12 mars 2001 | Rivero, C |

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

# RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2810138

N° d'enregistrement national

FA 593819
FR 0007318

| DOCUMENTS CONSIDÉRÉS COMME PERTINENTS | | Revendication(s) concernée(s) | Classement attribué à l'invention par l'INPI |
|---|---|---|---|
| Catégorie | Citation du document avec indication, en cas de besoin, des parties pertinentes | | |
| A | US 5 682 031 A (GERONIMI)<br>28 octobre 1997 (1997-10-28)<br>* colonne 2, ligne 8 - colonne 4, ligne 10; figures 1-3 *<br>----- | 1,8 | |

DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

| Date d'achèvement de la recherche | Examinateur |
|---|---|
| 12 mars 2001 | Rivero, C |

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

2

EPO FORM 1503 12.99 (P04C14)